Following Policy

and Reporting Incidents

You've probably heard "always follow policy" more times than you care to count. Indeed, we throw this phrase around a lot, and many organizations use it as a default slogan. And for good reason! Without policies, we invite chaos into our culture, which would undermine our efforts as workers and human firewalls. We would have no way to ensure the protection of sensitive data, and no way to know if we maintain compliance of various regulations. Worse yet, without policy, the likelihood of a security incident significantly increases.

We do everything we can to prevent security incidents. In fact, that's what following policy is all about: being *proactive* instead of *reactive*. But, despite our efforts, incidents will occur. How we respond to them is almost as important as how we prevent them. As the name suggests, incident response is identifying and reacting to a situation that puts our organization at risk in some manner. No matter what form the threat event comes in, reporting the event and responding in a timely manner could be the difference between a major breach or a minor setback.

So, don't think of policy as arbitrary rules thrust onto employees. Instead, view policy as a fundamental part of your job function—strategic procedures that were carefully designed and implemented to ensure the success of our organization.

What Should You Do?

Analyze each of the incidents outlined to the right. How would you handle them? What risks do they pose to our organization? Do you know how and where to report them?

Scenario 1

You receive an email that appears to come from a co-worker, but the grammar is odd and there's a sense of urgency within the message. There's also a link to an unfamiliar source that the sender begs you to click on.

Scenario 2

You find a USB drive in the parking lot far from the front door of our building. The drive is labeled with a sticker that says "financials", suggesting that it contains important, sensitive information.

Scenario 3

You notice a co-worker enter a secured area of our organization and hold the door open for someone that clearly doesn't have a badge or authorized credentials.

THE SOLUTION:

Report it! Each of the incidents above should be reported immediately. It is up to you to know how and to whom you should report incidents.
If you don't know, please ask!